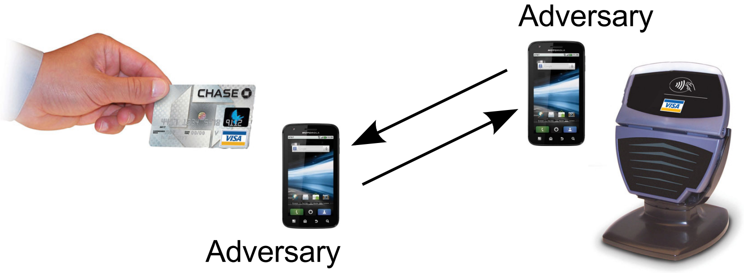
Analysis of the Proximity Check Protocol of Contactless Smartcards

Keywords: Security, Contactless Smartcard, RFID, Authentication, Relay Attacks, Distance-bounding

Goal: Check in practice the efficiency of the distance-bounding protocol of the Mifare DESFire contactless smartcard.



Level	Master in Computer Science (M2)
Academic Year	2018/19
Location	IRISA Rennes, France (www.irisa.fr)
Domain	Security and Cryptography
Supervisor	Gildas Avoine (www.avoine.net)
Required Skills	Programming in C, Linux, Experimental approach
Theory/Practice	Theory: 30%, Practice: 70%

Topic: Radio Frequency Identification (RFID) allows to identify objects or subjects without any physical nor optical contact, using transponders – micro-circuits with an antenna – queried by readers through a radio frequency channel. This technology is one of the most promising of this decade and is already widely used in applications such as access cards, transportation passes, payment cards, and passports. This success is partly due to the steadily decrease in both size and cost of passive transponders called *tags*. Contactless smartcards are RFID devices that benefit from more powerful capabilities. In this internship, the student will specifically focus on contactless smartcards.

The *relay attack* – sometimes referred to as *Mafia fraud* – exhibited by Desmedt, Goutier, and Bengio [1] recently became a major issue of concern for RFID authentication protocols. The adversary pretends to be the legitimate prover by relaying the messages that are exchanged during the execution of the protocol. This is illustrated through the following example. Consider an RFID-based ticket selling machine in a theater. To buy a ticket, the customer is not required to show his theater pass, an RFID tag. The customer needs to be close enough to the machine (verifier) so that the pass (prover) can communicate with it. The pass can be kept in the customer's pocket during the transaction. Assume there is a line of customers waiting for a ticket. Bob and Charlie masterminded the attack. Charlie is in front of the machine while Bob is far in the queue, close to Alice, the victim. When the machine initiates the transaction with Charlie's card, Charlie forwards the received signal to Bob who transmits it to Alice. The victim's tag automatically answers since a passive RFID tag – commonly used for such applications – responds without requiring the agreement of its holder. The answer is then transmitted back from Alice to the machine through Bob and Charlie who act as relays. The whole communication is transparently relayed and the attack eventually succeeds: Alice pays Charlie's ticket.

When it was first introduced in the late eighties, the relay attack appeared unrealistic. Nowadays, the relay attack is one of the most effective and feared attacks against RFID systems [2]. It can be easily implemented since the reader and the tag communicate wirelessly, and it is not easily detectable by the victim because queried (passive) tags automatically answer to the requests without agreement of their bearers. Relay attacks are for example used to steal cars in parking lots.

Distance-bounding protocols (see for example [3]) are promising solutions to prevent such relay attacks. These protocols measure the round-trip time of messages exchanged between the reader (verifier) and the tag (prover): if the round trip time is too long, then the reader considers the tag is outside its neighborhood and an attack running. There exist many distance-bounding protocols but most of them are theoretical proposals. The Mifare Plus and Mifare DESFire contactless smartcards are the only devices that take benefit of a distance-bounding protocol. The implemented protocol is however simpler than theoretical ones. The protocol so mitigates the problem but cannot fully avoid them. Consequently, this project will seek for the limits of the distance-bounding protocol implemented in these cards, especially the Mifare DESFire one.

The work will follow several steps:

1. Study the existing practical relay attacks and tools
2. Perform a relay attack on an ISO-14443 smartcard (off-the-shelf tools exist)
3. Learn how to communicate with a Mifare DESFire smartcard
4. Activate the Mifare DESFire distance-bounding protocol
5. Perform time measurements on the Mifare DESFire
6. Suggest improvements for the DESFire distance-bounding protocol

Laboratory: IRISA (*Institut de Recherche en Informatique et Systèmes Aléatoires*), founded in 1975, is a mixed research centre for IT, image, signal processing, and robotics, located in Rennes, France. The institute hosts 800 researchers belonging to 41 teams, and is funded by 7 entities, namely CNRS, ENS Rennes, Inria, INSA Rennes, Institut-Mines-Télécom, Supélec, Université de Bretagne Sud (UBS), and Université de Rennes 1. (www.irisa.fr)

Advisor: Gildas Avoine is a professor of Information Security and Cryptography at INSA Rennes in France. His research activities take place at IRISA, in Rennes (France), in the research group "Embedded Security and Cryptography" (EMSEC). Previously, he was a researcher at the MIT (USA) in the CSAIL, and at the EPFL (Switzerland) in the LASEC, where he obtained a PhD degree in cryptography. Gildas Avoine's main research area is information security, which he addressed with a cryptographic approach. His topics of interest include privacy models, lightweight authentication, distance-bounding protocols, cryptanalytic time-memory trade-offs, and forensics.

Contact:
Gildas Avoine (gildas.avoine@irisa.fr, www.avoine.net)
IRISA Rennes, Campus universitaire de Beaulieu (www.irisa.fr)
263 Avenue du Général Leclerc – CS 74205
F-35042 RENNES Cedex

References

1. Yvo Desmedt, Claude Goutier, and Samy Bengio. Special uses and abuses of the fiat-shamir passport protocol. In Carl Pomerance, editor, *Advances in Cryptology – CRYPTO'87*, volume 293 of *Lecture Notes in Computer Science*, pages 21–39, Santa Barbara, California, USA, August 1988. IACR, Springer-Verlag.
2. Gerhard Hancke. A practical relay attack on ISO 14443 proximity cards. Manuscript, February 2005.
3. Gerhard Hancke and Markus Kuhn. An RFID distance bounding protocol. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005*, pages 67–73, Athens, Greece, September 2005. IEEE, IEEE Computer Society.